National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
DataSoft Secure Tactical VPN Client for Android

Report Number: CCEVS-VR-VID11396-2023
Dated: August 14, 2023
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Randy Heimann
Lisa Mitchell
Linda Morrison
Clare Parran
Lori Sarem

Common Criteria Testing Laboratory

Raymond Smoley
Yoel Fortaleza
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation team of the evaluation of DataSoft Secure Tactical VPN Client for Android solution provided by DataSoft Corporation. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in August 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended, and meets the assurance requirements of the PP-Configuration for Application Software and Virtual Private Network (VPN) Clients, Version 1.3, 07 April 2023 which includes the Base PP: Protection Profile for Application Software, Version 1.4, 7 October 2021 (ASPP14) with the PP-Module for Virtual Private Network (VPN) Clients, Version 2.4, 31 March 2022 (VPNC24).

The Target of Evaluation (TOE) is the DataSoft Secure Tactical VPN Client for Android (SW version 2.3.7). The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the DataSoft Secure Tactical VPN Client for Android Security Target, Version 0.5, August 7, 2023 and analysis performed by the Validation team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	DataSoft Secure Tactical VPN Client for Android
Protection Profile	Protection Profile for Application Software, Version 1.4, 7 October 2021 (ASPP14) and the PP-Module for Virtual Private Network (VPN) Clients, Version 2.4, 31 March 2022 (VPNC24)
ST	DataSoft Secure Tactical VPN Client for Android Security Target, Version 0.5, August 7, 2023
Evaluation Technical Report	Evaluation Technical Report for DataSoft Secure Tactical VPN Client for Android, Version 0.4, August 7, 2023
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
Sponsor	DataSoft Corporation
Developer	DataSoft Corporation
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Randy Heimann, Lisa Mitchell, Linda Morrison, Clare Parran, Lori Sarem

Table 1: Evaluation Identifiers

3 Assumptions & Clarification of Scope

Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- Protection Profile for Application Software, Version 1.4, 7 October 2021 (ASPP14)
- PP-Module for Virtual Private Network (VPN) Clients, Version 2.4, 31 March 2022 (VPNC24)

That information has not been reproduced here and the ASPP14/VPNC24 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the ASPP14/VPNC24 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

Clarification of scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the Application Software Protection Profile with the VPNC module and performed by the Evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific Software Application and VPN Client models was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the ASPP14/VPNC24 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

4 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The TOE is the DataSoft Secure Tactical VPN Client for Android (SW version 2.3.7). The TOE enables remote users within an organization to communicate securely as if their devices were directly connected to a private network.

The TOE provides IPsec VPN client functionality for Android-based End User Devices (EUD) running on Android 11, Android 12, and Android 13 mobile devices (or "Platforms") running Linux Kernel earlier than v5.6.

The TOE complies with IKEv2 RFCs and can utilize X509v3 certificates for authentication of an IPsec peer. In a basic IPsec VPN connection, all traffic from the VPN client is encrypted and sent across the VPN gateway. Administrators can define profiles through the TOE or load them into a mobile device. Named profiles define the endpoints, authentication data, and cryptographic characteristics for a VPN connection. Profiles define the cryptographic configuration of the set of additional cryptographic options.

The TOE can interoperate with IKEv2 VPN Gateways but also includes extensions to route multicast traffic through the VPN, allowing the TOE to interoperate with DataSoft's small form factor Radio Access Point (RAP), which allows mobile and dismounted operators to perform C2-releated computing functions security across existing tactical communications networks.

4.1 TOE Evaluated Platforms

The TOE was specifically tested on those three different versions of Android using the following hardware:

Phone	Model	CPU	Kernel	Android OS
Samsung	S20 Tactical Edition	Qualcomm snapdragon 865 (SM8250)	4.19	Android 11
Google	Pixel 5	Qualcomm snapdragon 765G (SM7250)	4.19	Android 11
Google	Pixel 4a-5G	Qualcomm snapdragon 765G (SM7250)	4.19	Android 12
Google	Pixel 5a-5G	Qualcomm snapdragon 765G (SM7250)	4.19	Android 13

Table 2: Evaluated Platforms

4.2 TOE Architecture

The TOE product consists of a user space application installed as a standard Android APK.

4.3 Physical Boundaries

The TOE consists of a software-only VPN client application. The underlying mobile platform on which the TOE executes belongs to the IT environment.

5 Security Policy

This section summaries the security functionality of the TOE:

1. Cryptographic support
2. User data protection
3. Identification and authentication
4. Security management
5. Privacy
6. Protection of the TSF
7. Trusted path/channels

5.1 Cryptographic support

The TOE includes its own cryptographic library that implements approved cryptographic algorithms that the TOE uses to protect communication between itself and a VPN gateway over an unprotected network using IPsec. The TOE uses the Platform to protect credential data at rest.

The TOE platform provides asymmetric cryptography (Android's user keychain), which is used by the TOE for IKE peer authentication (using digital signature and hashing services). In addition, the TOE seeds its DRBG from the Platform.

5.2 User data protection

The TOE ensures that residual information from previously sent network packets processed through the platform are protected from being passed into subsequent network packets.

5.3 Identification and authentication

The TOE and TOE platform perform device-level X.509 certificate-based authentication of the VPN Gateway during IKE v2 key exchange. Device-level authentication allows the TOE to establish a secure channel with a trusted VPN Gateway. The secure channel is established only after each endpoint successfully authenticates each other.

5.4 Security management

The TOE provides all the interfaces necessary to manage the security functions identified throughout this Security Target. This includes interfaces to the user as well as to the VPN gateway. The IPsec VPN is fully configurable by a combination of functions provided directly by the TOE and those available to the associated VPN gateway. The TOE platform provides the functions necessary to securely update the TOE.

5.5 Privacy

The TOE does not store or transmit Personally Identifiable Information (PII) over a network.

5.6 Protection of the TSF

The TOE utilizes its own cryptographic functions to perform self-tests that ensure the TOE's integrity and algorithm correctness. The TOE platform provides the functions necessary to securely update the TOE software.

5.7 Trusted path/channels

The TOE establishes an IPsec trusted channel (which protects the transmitted data from unauthorized disclosure and modification) with a corresponding VPN gateway.

6 Documentation

The following documents were available with the TOE for evaluation:

- Secure Tactical VPN Client CC Configuration Guide, Version 1.1, July 26, 2023

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report for Secure Tactical VPN Client for Android, Version 0.4, August 7, 2023 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The Evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the ASPP14/VPNC24 including the tests associated with optional requirements.

8 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Secure Tactical VPN Client for Android TOE to be Part 2 extended, and to meet the SARs contained in the ASPP14/VPNC24.

8.1 Evaluation of the Security Target (ASE)

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the DataSoft Secure Tactical VPN Client for Android products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.2 Evaluation of the Development (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the ASPP14/VPNC24 related to the examination of the information contained in the TSS.

The Validation team reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.3 Evaluation of the Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The Validation team reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.4 Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was identified.

The Validation team reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the assurance activities in the ASPP14/VPNC24 and recorded the results in a Test Report, summarized in the AAR.

The Validation team reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.6 Vulnerability Assessment Activity (VAN)

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) on 7/18/2023 with the following search terms: “DataSoft Tactical Secure Mobility VPN Client”, “DataSoft Secure Tactical Mobility VPN Client”, “DataSoft Secure Tactical VPN Client”, “Secure Tactical VPN Client”, “DataSoft VPN Client”, “DataSoft Corporation”, “DataSoft”, “OpenSSL”, “Strongswan”.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.7 Summary of Evaluation Results

The Evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The Validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the Evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

9 Validator Comments/Recommendations

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Secure Tactical VPN Client CC Configuration Guide, Version 1.1, July 26, 2023 (AGD). No versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment need to be assessed separately, and no further conclusions can be drawn about their effectiveness.

10 Annexes

Not applicable.

11 Security Target

The Security Target is identified as: *DataSoft Secure Tactical VPN Client for Android Security Target, Version 0.5, August 7, 2023*.

12 Glossary

The following definitions are used throughout this document:

Term	Definition
Common Criteria Testing Laboratory (CCTL)	An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
Conformance	The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
Evaluation	The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
Evaluation Evidence	Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
Feature	Part of a product that is either included with the product or can be ordered separately.
Target of Evaluation (TOE)	A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
Validation	The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
Validation Body	A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

Table 3: Glossary

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] Protection Profile for Application Software, Version 1.4, 7 October 2021 (ASPP14).

[5] PP-Module for Virtual Private Network (VPN) Clients, Version 2.4, 31 March 2022 (VPNC24).

[6] DataSoft Secure Tactical VPN Client for Android Security Target, Version 0.5, August 7, 2023 (ST).

[7] Secure Tactical VPN Client CC Configuration Guide, Version 1.1, July 26, 2023. (AGD)

[8] Assurance Activity Report for DataSoft Secure Tactical VPN Client for Android, Version 0.4, August 7, 2023 (AAR).

[9] Detailed Test Report for DataSoft Secure Tactical VPN Client for Android, Version 0.4, August 7, 2023 (DTR).

[10] Evaluation Technical Report for DataSoft Secure Tactical VPN Client for Android, Version 0.4, August 7, 2023 (ETR)